

WHAT IS CLAIMED IS:

1 1. An account acquisition fraud management system, the account
2 acquisition fraud management system comprising:
3 a first analysis engine, wherein the first analysis engine is associated with a
4 first stored value product;
5 a second analysis engine, wherein the second analysis engine is associated
6 with a second stored value product; and
7 a cross monitor, wherein the cross monitor is operable to accept a first
8 transaction information from the first analysis engine and a second transaction information
9 from the second analysis engine, wherein the first transaction information is provided from
10 the cross monitor to the second analysis engine; and
11 wherein the second analysis engine is operable to reject a request for the
12 second stored value card product based at least in part on the first transaction information.

1 2. The system of claim 1, wherein the system further comprises:
2 a computer readable medium accessible to the cross monitor, wherein the
3 computer readable medium includes the first transaction information and the second
4 transaction information.

1 3. The system of claim 1, wherein the first transaction information is used
2 to create a transaction velocity.

1 4. The system of claim 1, wherein the first transaction information and
2 the second transaction information are selected from a group consisting of:
3 a physical address;
4 a telephone number;
5 a virtual address; and
6 a load source.

1 5. The system of claim 1, wherein the cross monitor is further operable to
2 maintain the first transaction information in a queue associated with an issuer of the second
3 stored value card product.

1 6. A method for detecting fraud in relation to stored value products, the
2 method comprising:

3 receiving a first suspicious activity indication from a first issuer analysis
4 engine, wherein the first issuer analysis engine is operable to monitor activities occurring in
5 relation to a first plurality of stored value products associated with the first issuer;
6 receiving a second suspicious activity indication from a second issuer analysis
7 engine, wherein the second issuer analysis engine is operable to monitor activities occurring
8 in relation to a second plurality of stored value products associated with the second issuer;
9 maintaining the first suspicious activity indication and the second suspicious
10 activity indication in a global negative file;
11 receiving an activity request from the first issuer analysis engine, wherein the
12 request includes a transaction information;
13 based at least in part on the transaction information, accessing the global
14 negative file; and
15 providing a response, wherein the response indicates the transaction
16 information is related to suspicious behavior.

1 7. The method of claim 6, wherein the transaction information is used to
2 create a velocity.

1 8. The method of claim 7, wherein the transaction information is selected
2 from a group consisting of:
3 a physical address;
4 a telephone number;
5 a virtual address; and
6 a load source.

1 9. The method of claim 6, wherein the transaction information is a
2 physical address.

1 10. The method of claim 6, wherein the transaction information is a
2 telephone number.

1 11. The method of claim 6, wherein the transaction information is a virtual
2 address.

1 12. The method of claim 6, wherein the response is maintained in a queue
2 associated with the first issuer.

1 13. The method of claim 12, wherein the response includes at least two of
2 the following:

3 a date of the suspicious behavior;
4 a funding account number;
5 a denial reason;
6 a review status; and
7 a reviewer note.

1 14. The method of claim 12, wherein the response includes an indication
2 of related accounts.

1 15. The method of claim 6, wherein the response is a first response
2 associated with a first account, wherein the global negative file indicates a second account
3 associated with the first account, and wherein the method further comprises:
4 providing a second response to the second issuer associated with the second
5 account.

1 16. A system for suppressing fraudulent activity in relation to account
2 acquisition, the system comprising:
3 a first load monitor associated with a first issuer;
4 a second load monitor associated with a second issuer;
5 a first enrollment monitor associated with the first issuer;
6 a second enrollment monitor associated with the second issuer; and
7 a cross monitor, wherein the cross monitor is operable to accept information
8 from one or more of the first load monitor, the second load monitor, the first enrollment
9 monitor and the second enrollment monitor, and wherein the cross monitor is operable to
10 communicate suspicious activity to both the first issuer and the second issuer.

1 17. The system of claim 16, wherein a request to load value on a stored
2 value product associated with the first issuer is processed at least in part by the first load
3 monitor.

1 18. The system of claim 17, wherein the first load monitor is operable to
2 apply a velocity check on a load request.

1 19. The system of claim 18, wherein the first load monitor is further
2 operable to compare the velocity with a predefined velocity limit.

1 20. The system of claim 19, wherein the first load monitor is operable to
2 provide a detected suspicious activity to the cross monitor.